Informacje cenne jak złoto

W zinformatyzowanej rzeczywistości dane medyczne (dalej DM) to nie tylko zapisy dotyczące przebiegu konkretnej choroby. W dokumentacji tej znajdują się też informacje na temat stanu zdrowia pacjenta w przeszłości i takie, które mogą ułatwić ocenę jego zdrowia w przyszłości. Dane te mają niezwykłe znaczenie w ochronie prywatności danej osoby, a równocześnie są niezbędne w trakcie leczenia.

Nie jest przesadą, że mówiąc o ochronie danych medycznych, mówimy o ochronie zdrowia i życia pacjentów. Dlatego są one chronione wieloma przepisami od konstytucji (art. 51.) począwszy, na rozporządzeniach do ustaw skończywszy.

Zmiana świadomości

Jedną z najistotniejszych kwestii jest ochrona dostępu do DM. Największe zagrożenie związane z ich przetwarzaniem jest zaś takie, że trafią w niepowołane ręce. Pokusa wykorzystana danych w celu zwiększenia dochodów (np. przez firmy farmaceutyczne lub ubezpieczeniowe) sprawia, że jest na nie duży popyt. Zresztą nieuprawniony dostęp nie musi wynikać z zaplanowanego działania naruszającego prawo. Wyciek z systemu informatycznego może być po prostu konsekwencją niedbałego przetwarzania i nienależytego zabezpieczenia danych.

Jak sobie z tym radzić? Wymienione problemy są najczęściej następstwem ustanowienia zbyt dużego dostępu do DM. Tymczasem powinien on wynikać ze stosowania zasady, którą w języku angielskim określa się jako *need to know*, czyli dostęp tylko dla tych, którzy rzeczywiście tego potrzebują.

Na pytanie, do jakich danych powinien mieć dostęp konkretny pracownik służby zdrowia, oczywiście nie odpowie informatyk, tylko lekarz. Informatyk podpowie natomiast, że można stworzyć kilka lub kilkanaście profilów dla poszczególnych grup pracowników służby zdrowia (lub innych, którym dane są udostępniane). I tak pielęgniarki będą miały dostęp tylko do tych danych, które są im niezbędne do wykonywania pracy. Inne uprawnienia musi mieć lekarz specjalista, a jeszcze inne pracownik administracyjny szpitala.

Sytuacje wyjątkowe

Przy ustalaniu zasad dostępu warto pamiętać o uwzględnieniu czynnika czasu i o sytuacjach wyjątkowych. Jeśli chodzi o okres dostępu, to zapewne informacje o stanie zdrowia pacjentów, którzy przebywali w placówce służby zdrowia wiele lat temu, nie są szczególnie istotne i możemy dostęp do nich maksymalnie ograniczyć (np. poprzez wyłączenie możliwości wyświetlania danych starszych niż zaproponowany okres). Oczywiście przypadki szczególne, pomagające w prowadzeniu podobnych terapii u innych chorych, mogą być nadal dostępne. Podczas leczenia mamy też do czynienia z sytuacjami wyjątkowymi, kiedy konieczny jest natychmiastowy dostęp do danych, a dodatkowo musi mieć w nie wgląd osoba na co dzień do tego nieuprawniona (np. telefoniczne konsultacje lekarza uczestniczącego w akcji ratunkowej). Na wypadek takich sytuacji powinniśmy mieć specjalną procedurę, z której użycia dokonamy rozliczenia.

Rozliczalność dostępu

Z prawem dostępu nierozerwalnie łączy się konieczność zapewnienia tzw. rozliczalności. Oznacza to, że system powinien zapewniać możliwość kontroli. To nie tylko obowiązek. Takie zasady mogą być niezwykle pożyteczne. Wyobraźmy sobie, że w kartotece znajdujemy informację o nowatorskim zabiegu, który zdecydowanie poprawił jego stan zdrowia. Ileż bardziej pomocna będzie ta informacja, jeśli będziemy wiedzieli, kto taki zabieg przeprowadził. Konsultacja z tym lekarzem może się okazać niezwykle pomocna.

W rozporządzeniu o ochronie danych osobowych znalazły się zapisy poświęcone tym wymogom, wyszczególniające elementy, które muszą się znaleźć w systemie:

- data pierwszego wprowadzenia danych do systemu,
- identyfikator użytkownika wprowadzającego dane osobowe, chyba że dostęp do systemu informatycznego i przetwarzanych danych ma tylko jedna osoba,
- źródła danych, w wypadku zbierania danych nie od osoby, której one dotyczą,
- informacje o odbiorcach, którym dane osobowe zostały udostępnione, data i zakres tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych.

Pierwsze dwa warunki powinny być zrealizowane automatycznie po zatwierdzeniu operacji wprowadzenia danych (to wymóg rozporządzenia). Warto wspomnieć, że warunków, jakie powinien spełniać system informatyczny, w którym przetwarzane są DM, jest więcej. DM to szczególnie chronione dane osobowe, określane jako wrażliwe i przetwarzanie ich objęte jest dodatkowymi warunkami. Aby wiedzieć, czy system spełnia te wymogi, warto skorzystać z prac organizacji ISACA, która kilka lat temu opracowała SurvivalKit, czyli wytyczne do audytu i kontroli systemów informatycznych pod kątem zgodności z ustawą o ochronie danych osobowych (www.isaca.org.pl; w zakładce Projekty, a następnie Zamknięte projekty).

Dodatkowym zagadnieniem związanym z dostępem do DM i jego rozliczalnością jest udostępnianie ich do celów naukowo-badawczych. W takich wypadkach mamy do czynienia zazwyczaj z dwoma typami informacji – ze zbiorczą informacją statystyczną oraz szczegółową informacją na temat konkretnych przypadków leczenia. W pierwszym wypadku sprawa jest prostsza – należy przekazywać tylko informacje zbiorcze, podając dane statystyczne zgodnie z profilem zapytania. Najlepiej, jeśli system umożliwia generowanie wcześniej zdefiniowanych raportów. W drugim wypadku jest niezwykle istotne, aby dokonać pełnej anonimizacji danych. Na podstawie udostępnionych danych osoba, która je uzyskała, nie powinna móc ustalić, kogo one dotyczą.

Należy zwrócić uwagę, że anonimizacja danych nie może być realizowana poprzez wymieszanie przypisania DM losowym osobom w bazie danych. Fałszywa informacja, że ktoś może być chory na jakąś chorobę jest równie niebezpieczna w ochronie prywatności jak prawdziwa. Najlepszym sposobem jest usunięcie wszelkiego rodzaju danych.

MIROSŁAW MAJ

Autor jest szefem polskiego zespołu ds. reagowania na naruszenia bezpieczeństwa w internecie (NASK/CERT)